Remarks/Arguments

Claims 1 - 20 are pending. No amendments to the claims have been made. Reconsideration of this application is requested.

35 USC 103 Claim Rejections

Claims 1 and 12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent No. 5,689,559 issued to Park (Park Patent) in view of United States Patent No. 5,796,826 also issued to Park (Park '826 Patent). Claims 2–7 and 13-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Park in view of Park '826 and further in view of Mandelbaum (United States Patent No. 5,544,246). Claims 8–11 and 15-19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Park in view of Park '826 and further in view of Mandelbaum and EBU ("Functional model of a conditional access system", EBU Project Group B/CA). Claim 20 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Park in view of Park '826 and further in view of EBU. Applicant respectfully traverses these rejections for at least the following reasons.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. Further, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j).* Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. As discussed below, the cited prior art references, both singly and in combination, fail to teach or suggest all of the limitations of Claims 1 - 20.

Claims 1 - 11

Claim 1 recites:

> A method for copying a program having a scrambled program content component and an encrypted control component comprising:
>
> (a) receiving, in a recording apparatus, said program;
>
> (b) attaching a data item to said encrypted control component, said data item indicating that said program has been copied;
>
> (c) encrypting said encrypted control component and said data item to generate a nested control component; and
>
> (d) recording said program content component and said nested control component. (emphasis added)

Thus, Claim 1 broadly encompasses: (a) receiving a program having scrambled content and an encrypted control component; (b) attaching a data item indicating that the program has been copied to the encrypted control component; (c) encrypting the already encrypted control component and attached data item to generate a nested control component; and (d) recording the program content and nested control component. The Park and Park '826 patents, both singularly, and in combination, fail to teach or suggest at least the limitations of (1) attaching a data item to said encrypted control component, said data item indicating that said program has been copied and (2) encrypting the encrypted control component and data item to generate a nested control component.

An encrypted "nested" control component according to the present invention comprises a control component having a data item attached thereto and encrypted. For example, page 8, line 28 – page 9, line 2 of the present specification recites:

> In one embodiment of the present invention if the content is scrambled, the recorder encrypts the ECMs using the global public key. Before encryption takes place, the recorder attaches a mark (or data item) (see Figure 2b) to each ECM as an indication of copying. *In general, every time a scrambled movie is copied, its ECMs are encrypted once again, a process that may be referred to as "nesting".* This allows the smartcard to determine how many times the original movie has been copied. The following example (wherein GPK is the Global public key, E is the Encryption process, CW is the Control word (the key for descrambling) and ECM contains CW, CCI, source of the content and other data) detects an illegitimate copy and prevents the display thereof.
>
> Assume an ECM of the movie has the form: E_{GPK}(CW, never-copy). *If a recorder receives this ECM. it will transform it to: E_{GPK} [E_{GPK}(CW, never-copy), copy-mark)]. The movie with this nested ECM will be the output of the recording process.*

Thus, a received ECM E_{GPK}(CW, never-copy) is again encrypted along with a data item to generate a nested control component E_{GPK} [E_{GPK}(CW, never-copy), copy-mark)]. The received ECM remains intact, and is fit or placed into some thing else – namely for the received ECM E_{GPK}(CW, never-copy), E_{GPK} [… , copy-mark)]. When an illegitimate copy of a legitimate copy is created according to an aspect of the present invention, the ECM will have two layers of nesting [E_{GPK} {E_{GPK} [E_{GPK}(CW, copy-once), copy-mark)], copy-mark}]. *See, specification, page 9, lines 6-9.*

In an exemplary embodiment, each time a scrambled movie is copied its ECMs are again encrypted, thereby allowing the system to determine how many times the original movie has been copied by examining the nested nature of the ECMs. *See, e.g., specification, page 8, line 31 - page 9, line 9.* In contrast, the cited art of record fails to teach or even suggest, the subject matter as claimed in present claim 1.

In response to Applicant's previous response, the Final Office action argues that, contrary to Applicant's assertions, Park '826 *teaches generating a nested control component. See, 6/3/2005 Office action, pars. 17, 18.* To support this assertion, the Office action argues Park '826 teaches:

> a control component (i.e. scrambling key, fig 7, m), where an exclusive-or operation is performed on scrambling key and additional information (i.e., generating encrypted control component, see column 4, lines 52-53), *and the encrypted control component which includes the scrambling key and data item is further encrypted with another exclusive-or operation with key matrix R (i.e., generating nested control component*, see column 4, lines 53-57). (*emphasis added).*

Applicant respectfully disagrees. An examination of Park '826 shows that Park '826 simply fails to teach or suggest the limitations alleged. In that regard, attention is directed to Column 4, lines 52-57 of Park '826 which discuss the apparatus of Fig. 7. In Fig. 7 of Park '826, the vector matrix mG formed from the scrambling key vector (m) and matrix (G) are subjected to an exclusive-or operation with an additional information vector (v) by adder 12 to provide an intermediate resultant vector $b^{(i)}$. *See, col. 4, lines 52-53.* The truth table for an exclusive-or operation is:

mG	v	$b^{(i)}$
0	0	0

0	1	1
1	0	1
1	1	0

as is demonstrated by the excerpt from section 5-5-8 of the textbook, Modern Digital Design, by Richard S. Sandige (copyright 1990), appended to this response as Attachment "A". Thus, the scrambling key vector matrix mG is compared with the additional information vector v, and where they differ, the resultant is set in the intermediate resultant vector $b^{(i)}$. The intermediate resultant vector $b^{(i)}$ is then subjected to an exclusive-or operation with a weight randomization matrix (R) by matrix multiplier 13. This results in a weight randomized version of $b^{(i)}$ being provided as vector $d^{(i)}$. *See, col. 4, lines 53-57.*

The above-identified passages teach at most scrambling the additional information vector v using a scrambling key vector matrix mG to generate an intermediate resultant vector $b^{(i)}$, and then weight randomizing the scrambled intermediate resultant vector $b^{(i)}$ to provide a weight randomized vector $d^{(i)}$, e.g., ciphertext $d^{(i)}$. Thus, Park '826 clearly fails to teach or suggest a "nested" approach for generating a "nested control component" as recited in present Claim 1. This is confirmed by the Park '826 teaching of updating its "additional information", in contrast to "attaching a data item to said encrypted control component, said data item indicating that said program has been copied; and encrypting said encrypted control component and said data item to generate a nested control component" as recited in present Claim 1.

More particularly, the relied upon excerpts of Park '826 do not teach to: (1) attach any information to an already encrypted control component; nor (2) again encrypt an already encrypted control component with any attached data in order to generate a nested control component; since the relied upon Park '826 intermediate vector $b^{(i)}$ has no additional data attached to it, and is instead merely weight randomized by the weight randomization matrix (R). Accordingly, Applicant traverses any assertion of the Final Office action that Park '826 teaches, or suggests, generating a nested control component as recited in present Claim 1.

Applicant again notes that the Office Action acknowledges the primary Park reference fails to teach or suggest "encrypting the encrypted control component and said data item to generate a nested control component" as recited in Claim 1. As discussed herein, the Park '826 reference fails to cure the deficiencies of the primary Park reference as applied to Claim 1. Park '826 (similar to the Park primary reference) merely encrypts an unencrypted control word (i.e. scrambling key) along with an **updatable** value (i.e. additional information) where, upon decryption of the encrypted scrambling key and the updatable value (see FIG. 8 of Park '826), that value itself is updated (i.e. decremented) and then recorded onto the video tape.

Park '826 discloses an encrypting portion 10 (Fig. 7, column 4, line 46), in which additional information containing a reproducible number is encrypted together with a scrambling key. *See, e.g., Park '826, Col. 6, lines 62 - 64.* However, this additional information and scrambling key are in no way encrypted to generate a nested control component as recited in Claim 1.

In contrast, a detailed reading of column 2, lines 53-60 of Park '826 reveals:

> In playback of video tape, a decryption algorithm corresponding to the encryption algorithm is used to restore a scrambling key and information on a reproducible number remaining. Using the restored scrambling key, the original bit stream is restored through descrambling. Here, the reproducible number remaining is reduced by one and then recorded on video tape. (emphasis added).

Column 6, lines 62-65 of Park '826 further reveals:

> "In encrypting portion 10, the additional information containing the reproducible number is encrypted together with the scrambling key. In Decrypting portion 20, the additional information is updated for every playback". (emphasis added).

From these passages, it is clear that Park '826 does not generate a nested control component as recited in the present claims, but instead merely encrypts a scrambling key along with an updatable value (i.e. additional information). The scrambling key is then decrypted by decrypting portion 20 (Fig. 8), as is the updateable value, which is then modified (i.e. decremented) and recorded onto the video tape for each playback.

Figures 13A – 13F of Park '826 illustrate the process for updating ciphertext $d_{(i)}$ to indicate a videotape reproduction of the content. Video tape travels in a manner such that it cannot be updated at the very position from which it is read. As shown in col. 8, lines 30-52, Park '826 proposes reading $d_{(i)}$ from one repetition code symbol and then updating, e.g., recording or replacing, the next repetition code symbol with $d_{(i+1)}$.

According to the Park '826 reference, the repetition code states of $d_{(i)}$ and $d_{(i+1)}$ correspond to a repetition code of i+1 times.

Thus, Park '826, like the Park reference, merely teaches replacing or recording over a previous copy marker with a current copy marker, and not "encrypting [an already] encrypted control component and said data item to generate a nested control component" as is recited by Claim 1.

Accordingly, as Park and Park '826 each fail to teach or suggest the recited "encrypting said encrypted control component and said data item to generate a nested control component" of Claim 1, clearly their combination also fails to teach or suggest such a feature. For the foregoing reasons, Applicant respectfully requests reconsideration and removal of this 35 USC 103 rejection of Claim 1.

For purposes of completeness, Applicant submits Mandelbaum and EBU fail to cure the deficiencies of both the Park and Park '826 references. Reconsideration and removal of the rejections of dependent Claims 2 – 11 is requested.

Claims 12 - 19

In similar fashion, independent method Claim 12 recites "receiving said restricted program in a processing apparatus, said restricted program having a scrambled program content component and a nested control component." The arguments discussed herein with regard to the cited art relative to present Claim 1 also apply to independent method Claim 12. As the cited art, both singularly, and in combination, fail to teach or suggest a nested control component (e.g., an encrypted, encrypted control component and data item like E_{GPK} [E_{GPK}(CW, never-copy), copy-mark)]), Applicant submits they analogously fail to teach receiving such a nested control component. Accordingly, Applicant respectfully requests reconsideration and removal of this 35 USC 103 rejection and allowance of independent Claim 12.

For purposes of completeness, Applicant submits Mandelbaum and EBU fail to add anything to the Park and Park '826 Patents in this regard. Accordingly, Applicant further requests reconsideration and removal of the rejections of Claims 13 – 19, at least by virtue of these Claims' ultimate dependency from a patentably distinct base Claim 12.

Claim 20

Claim 20 analogously recites a "restricted program having a scrambled audio/video component and a nested control component." As the cited art, both singularly, and in combination, fail to teach or suggest a nested control component (e.g., an encrypted, encrypted control component and data item like E_{GPK} [E_{GPK}(CW, never-copy), copy-mark)]), Applicant submits they analogously fail to teach a restricted program having a nested control component. For purposes of completeness, Applicant submits EBU fails to add anything to the Park and Park '826 Patents in this regard. Accordingly, Applicant respectfully requests reconsideration and removal of this 35 USC 103 rejection of Claim 20.

CONCLUSION

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding remarks, this application stands in condition for allowance. No fee is believed due in regard to the present response. However, if a fee is due, please charge the fee to Deposit Account 07-0832. Accordingly then, reconsideration and allowance are respectfully solicited.

If, however, the Examiner is of the opinion that such action cannot be taken, (1) the Examiner is invited to contact the Applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled, and (2) entry of this response for purposes of preparing the record for ex-parte appeal is respectfully requested.

Respectfully submitted,

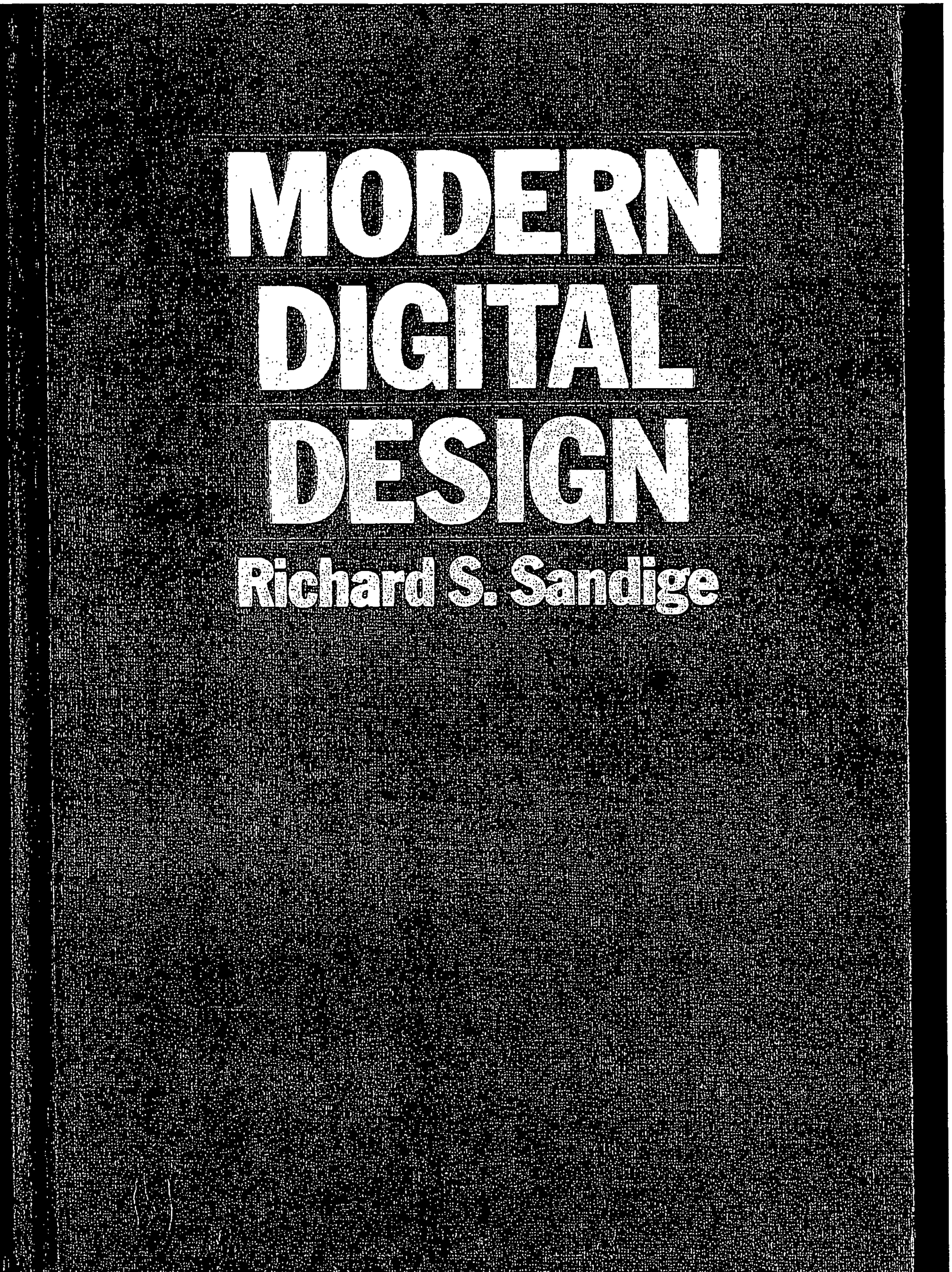
Eskicioglu et al.

By:

Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: August 25, 2005



MODERN DIGITAL DESIGN

Richard S. Sandige

This book was set in Times Roman by Publication Services.
The editors were Alar E. Elken and John M. Morriss;
the production supervisor was Friederich W. Schulte.
The cover was designed by Joseph Gillians.
Project supervision was done by Publication Services.
R. R. Donnelley & Sons Company was printer and binder.

MODERN DIGITAL DESIGN

3 4 5 6 7 8 9 0 DOC DOC 9 5 4 3 2 1

ISBN 0-07-054857-9

Library of Congress Cataloging-in-Publication Data

Sandige, Richard S.
Modern digital design / Richard S. Sandige.
p. cm.—(McGraw-Hill series in electrical engineering. Computer engineering)
Includes bibliographies and index.
ISBN 0-07-054857-9
1. Logic circuits—Design and construction. 2. Logic design.
I. Title. II. Series.
TK7868.L6S26 1990
621.39'5—dc20 89-12401

line MUX shown in

lexer is shown below.
ble, if written without

iat the 4-to-1 line MUX
X discussed earlier.
plexer can be checked by
ght side of the function,
F agrees with the output
vritten directly from the

Selectors can also be
ocedure is to use block
they can be connected
or example, using three
constructed as shown
time of $4t_{pd}$ compared
ıltiplexer design shown

ie 4-to-1 line Multiplexer
er.

tiplexer is shown in Fig.

plexer selects each of the
r select inputs SI4 SI3 =
or select inputs SI4 SI3 =
selected, then select inputs
cted for n = 0 0 0 through

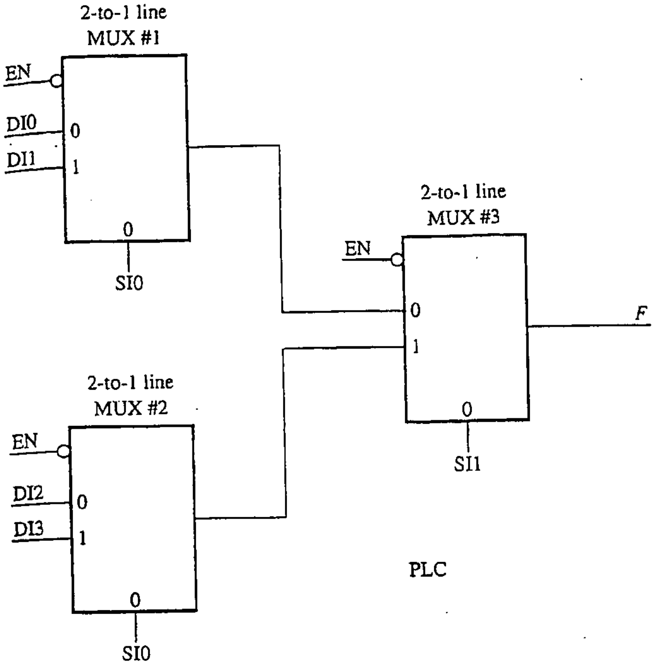


FIGURE 5-23
A 4-to-1 line Multiplexer constructed from three 2-to-1 line Multiplexers.

1 1 1 for each respective MUX. The overall data input selected is determined by concatenating the binary values for *m* and *n*.

5-5-8 Exclusive OR and Exclusive NOR

Exclusive ORs and Exclusive NORs are special two-input devices that are obtained from the definition of their respective truth table logic descriptions. The truth table description for these devices are listed as follows:

X	*Y*	*F*1
0	0	0
0	1	1
1	0	1
1	1	0

X	*Y*	*F*2
0	0	1
0	1	0
1	0	0
1	1	1

By definition, *F*1 is an Exclusive OR function, and its complement *F*2 is an Exclusive NOR function. The Karnaugh maps for *F*1 and *F*2 are shown in Fig. 5-24. Neither function can be reduced.